Sub a1

What is claimed is:

1. A method of provisioning a user's broadband telephony interface comprising the steps of:

receiving information authenticating a provisioning server;

establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server; and

encrypting and transmitting a cryptographic key associated with the user to the provisioning server.

2. The method of claim 1 wherein the communication channel is a voice channel connection.

3. The method of claim 2 wherein the communication channel is encrypted using an audio channel key which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

4. The method of claim 3 wherein the cryptographic key associated with the user is encrypted using a session key which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

5. The method of claim 4 wherein the session key and the audio channel key are encrypted using a cryptographic key that is encrypted using a cryptographic key associated with the provisioning server and transmitted to the provisioning server with the encrypted session and audio channel key.

6. The method of claim 5 wherein the cryptographic key associated with the provisioning server is received with the information authenticating the provisioning server.

7. The method of claim 6 wherein a random nonce is included with the encrypted session key.

8. The method of claim 1 wherein the information authenticating the provisioning server is a digital certificate.

9. The method of claim 1 wherein the cryptographic key associated with the user is a symmetric key.

10. The method of claim 1 wherein the cryptographic key associated with the user is a public key corresponding to a private key stored in the broadband telephony interface.

11. The method of claim 1 wherein a hash is included with each transmission.

12. A broadband telephony interface comprising:

a first interface to a user telephone;

a second interface to a communication network with access to a provisioning server;

memory for storing cryptographic keys;

a processor connected to the memory and the first and second interfaces for executing program instructions, the program instructions causing the processor to perform the steps of:

receiving information authenticating the provisioning server;

establishing a communication channel between the user telephone and the provisioning server over which is transmitted authorization information from the user to the provisioning server; and

encrypting and transmitting a cryptographic key associated with the user to the provisioning server.

13. The broadband telephony interface of claim 12 wherein the communication channel is a voice channel connection.

14. The broadband telephony interface of claim 13 wherein the communication channel is encrypted using an audio channel key which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

15. The broadband telephony interface of claim 14 wherein the cryptographic key associated with the user is encrypted using a session key which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

16. The broadband telephony interface of claim 15 wherein the session key and the audio channel key are encrypted using a cryptographic key that is encrypted using a cryptographic key associated with the provisioning server and transmitted to the provisioning server with the encrypted session and audio channel key.

17. The broadband telephony interface of claim 16 wherein the cryptographic key associated with the provisioning server is received with the information authenticating the provisioning server.

18. The broadband telephony interface of claim 17 wherein a random nonce is included with the encrypted session key.

19. The broadband telephony interface of claim 12 wherein the information authenticating the provisioning server is a digital certificate.

20. The broadband telephony interface of claim 12 wherein the cryptographic key associated with the user is a symmetric key.

21. The broadband telephony interface of claim 12 wherein the cryptographic key associated with the user is a public key corresponding to a private key stored in the broadband telephony interface.

22. The broadband telephony interface of claim 12 wherein a hash is included with each transmission.

23. A method of operating a provisioning server comprising the steps of:

receiving a request to be provisioned from a broadband telephony interface;

transmitting authentication information to the broadband telephony interface;

receiving authorization information over a communication channel established between a user of the broadband telephony interface and the provisioning server; and

receiving an encrypted cryptographic key associated with the user from the broadband telephony interface.

24. The method of claim 23 wherein the communication channel is a voice channel connection.

25. The method of claim 24 wherein the communication channel is encrypted using an audio channel key which is received from the broadband telephony interface prior to establishing the communication channel.

26. The method of claim 25 wherein the cryptographic key associated with the user is encrypted using a session key which is received from the broadband telephony interface prior to establishing the communication channel.

27. The method of claim 26 wherein a cryptographic key associated with the provisioning server is transmitted to the broadband telephony interface and the session key and the audio channel key are received encrypted using the cryptographic key associated with the provisioning server.

28. The method of claim 27 wherein the cryptographic key associated with the provisioning server is transmitted with the authentication information to the broadband telephony interface.

29. The method of claim 28 wherein a random nonce is included with encrypted session key and audio channel key.

30. The method of claim 23 wherein the authentication information is a digital certificate.

31. The method of claim 23 wherein the cryptographic key associated with the user is a symmetric key.

32. The method of claim 23 wherein the cryptographic key associated with the user is a public key corresponding to a private key stored in the broadband telephony interface.

33. The method of claim 23 wherein a hash is included with each transmission.